

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1-13. (cancelled).

14. (new) An authentication system for providing authentication of data communication, comprising:

an authentication string applied once to a communal string field of a simple network management protocol message to be transmitted in a communication link between a client and an agent, the authentication string based on a shared seed between the client and the agent, the authentication string determined by a substantially similar algorithm at both the client and the agent using the shared seed.

15. (new) A system according to claim 14, further comprising:

an authenticity checking program installed in a receiving one of the client and the agent for checking authenticity of the authentication string by checking the authentication string received in the simple network management protocol message against the authentication string determined by

the algorithm program at the receiving one of the client and the agent.

16. (new) A system according to claim 14, wherein,
the simple network management protocol message comprises three parts including i) a protocol version, ii) the communal string field, and iii) a data area divided into protocol data units,

the communal string field is a simple network management protocol community identifier,

the communal string field is stored as a character string.

17. (new) A system according to claim 16, wherein
the simple network management protocol message applies ASN-1 encoding, and

the algorithm at both the client and the agent is based on one of MD2, MD4, and MD5.

18. (new) A system according to claim 14, further comprising:

another authentication string applied once to the communal string field of a simple network management protocol message, the another authentication string based on the shared seed between the client and the agent, the another authentication

string determined by the substantially similar algorithm at both the client and the agent using the shared seed,

wherein the another authentication string is determined subsequent to the authentication string being applied to the communal string field.

19. (new) A system according to claim 15, wherein, each of the client and the agent are configured as both a message transmitting network entity and a message receiving network entity,

each of plural messages transmitted between the client and the agent includes a different authentication string,

for each of the plural messages, the authenticity checking program installed in the receiving one of the client and the agent verifies that the authentication string received in the simple network management protocol message matches the authentication string determined by the algorithm program at the receiving one of the client and the agent.

20. (new) A system according to claim 14, wherein, the shared seed is based on a random number generator, both the client and the agent include one of the random number generator, and

the shared seed is generated at one of the client and the agent and then communicated to the other of the client and the agent.

21. (new) A system according to claim 14, wherein the communication link comprises the Internet.

22. (new) A system according to claim 14, wherein the algorithm generates a new authentication string based on the seed and based on a secure random logic for being difficult to copy a pattern of a plurality of the authentication strings.

23. (new) A system according to claim 14, wherein the client and the agent remain synchronized in an operation loop of currently generated and once applied authentication strings by an acknowledgement message between the client and the agent.

24. (new) A system according to claim 15, wherein,
one of the client and the agent sets an operation in accordance with the data communication unauthorized when the authentication string in the received message does not correspond with the authentication string determined by the algorithm program at the receiving one of the client and the agent, and

each of the client and the agent are configured as both a message transmitting network entity and a message receiving network entity.

25. (new) An apparatus for providing authentication of data communication over a communication link between a client and an agent in accordance with a simple network management protocol, comprising:

a component generating an authentication string adapted to be applied once to a communal string field of a simple network management protocol message to be transmitted in a communication link between the client apparatus and the agent apparatus, the authentication string based on a shared seed between the client apparatus and the agent apparatus, the component comprising a substantially similar algorithm at both the client apparatus and the agent apparatus using the shared seed.

26. (new) An apparatus according to claim 25, further comprising:

an authenticity checking component installed in a receiving one of the client apparatus and the agent apparatus for checking authenticity of the authentication string by checking the authentication string received in the simple network management protocol message against the authentication string

determined by the algorithm program at the receiving one of the client apparatus and the agent apparatus.

27. (new) An apparatus according to claim 25, wherein, the simple network management protocol message comprises three parts including i) a protocol version, ii) the communal string field, and iii) a data area divided into protocol data units, and

the communal string field is a simple network management protocol community identifier.

28. (new) A method for authentication of data communication over a communication link between a transmitting network entity and a receiving network entity in accordance with a simple network management protocol, the method comprising:

establishing a seed at a first one of a transmitting network entity and a receiving network entity;

sharing the established seed with a second one of the transmitting network entity and the receiving network entity;

generating an authentication string to be applied once based on the shared seed at both the transmitting network entity and the receiving network entity;

incorporating, at the transmitting network entity, the generated authentication string into a communal string field of a

Simple Network Management Protocol message for transmitting the message in accordance with simple network management protocol;

receiving the message at the receiving network entity;

at the receiving network entity, checking the authentication string of the communal string field of the message for correspondence with the authentication string generated at the receiving network entity, and

authenticating the message when there is a correspondence between the authentication string of the communal string field of the message and the authentication string generated at the receiving network entity.

29. (new) A method according to claim 28, further comprising:

generating another authentication string to be applied once based on the shared seed at both the transmitting network entity and the receiving network entity;

incorporating, at the transmitting network entity, the another authentication string into the communal string field for transmitting another message in accordance with the simple network management protocol;

receiving the another message at the receiving network entity;

checking the another authentication string of the communal string field of the another message for correspondence

with the another authentication string, generating at the receiving network entity; and

authenticating the another message when there is a correspondence between the another authentication string of the communal string field of the another message and the generated another authentication string at the receiving network entity.

30. (new) A method according to claim 28, wherein, each of the transmitting network entity and the receiving network entity include both a client and an agent and are configured to operate as both the client and the agent.

31. (new) A method according 28, wherein, the simple network management protocol message comprises three parts including i) a protocol version, ii) the communal string field, and iii) a data area divided into protocol data units,

the communal string field is a simple network management protocol community identifier, and

said step of sharing the established seed with the second one of the transmitting network entity and the receiving network entity, the shared seed is generated by a random number generator program and the seed is contained in one of the protocol data units of the simple network management protocol message.

32. (new) A method according to claim 28, wherein,
the simple network management protocol message
comprises three parts including i) a protocol version, ii) the
communal string field, and iii) a data area divided into protocol
data units, and

the communal string field is a simple network
management protocol community identifier.

33. (new) A method according to claim 32, wherein,
the simple network management protocol message applies
ASN-1 encoding,

the communal string field is stored as a character
string, and

the algorithm is based on one of MD2, MD4, and MD5.